ACTIVITY REPORT

NAADSN
North American and Arctic Defence and Security Network

naadsn.ca

April 14, 2020
CDA Conference Report

Report of the Ottawa Conference on Security and Defence: *Stickhandling Through Roughing and Interference: How to Position Canada in the Great Power Plays*

Nancy Teeple, PhD
NAADSN Post-doctoral Fellow

CDA Conference hosted by the Conferences of Defence Associations Institute (CDAI)
4-5 March 2020, Chateau Laurier, Ottawa

Purpose

The aim of this report is to present a review of the issues addressed in the conference sessions, drawing out important themes in a descriptive analysis of their application to Canadian defence and security, highlighting significant issues of concern, and identifying gaps and areas requiring further exploration.

Background

The CDA Institute[1] annual Conference features high-level keynote speakers, such as the Prime Minister of Canada, the Minister of National Defence, the Chief of Defence Staff, and currently and former advisors to national leadership. Participation in CDAI events facilitates knowledge exchange through experts' presentations on specialized topics and follow-up discussion sessions with an interested audience. Networking coffee breaks and lunches are also important parts of the professional development opportunity provided at these for a – a context for access to expertise and unstructured discussion not otherwise available to emerging next generation scholars.

Event Description

The Ottawa Conference on Security and Defence is an annual forum hosted by CDAI to address pressing security and defence issues for Canada and its allies. This event provides engagement among the "community of thought leaders on the future of Canadian security and defence."[2] In attendance were academics, government and think-tank analysts, military commanders, officers, and NCOs, graduate students, and media journalists. Keynotes and sessions (moderated panel discussions) addressing thematic issues featuring the foremost Canadian and international experts on specific defence and security topics.[3] This year's sessions addressed the following:

1) Session 1: Escalating or De-escalating with Russia Relations: NORAD Modernization, Forward Presence, and Re-vamping the Arms Control Treaty Architecture.
2) Session 2: Great Power Dynamics in the Middle East.
3) Session 3: Global Transatlantic Cooperation.
4) Session 4: Designating Procurement: Future Challenges and Getting the Right Equipment at the Right Price at the Right Time.
5) Session 5: Military Personnel: Recruiting and Retaining the Future Soldier.
6) Session 6: Cyber/5G – Critical Infrastructure and Battlefield Threats.
7) Session 7: Moving Forward: How is Canada to Position Itself to Secure its National Interests in an Age of Great Power Competition and Warfare Below the Threshold?
8) Session 8: The Future of War.

The issues addressed in each session tended to overlap with others, which enriched discussion and demonstrated how developments in different domains, geopolitical regions, and actors influence one another. The experts identified problems in Western understanding of security threats and provided recommendations on how to better identify the threat, understand where we are at, and respond.

The following discussion organizes the sessions' material into subject catetories and does not attribute statements to any one panelist. Rather, the material is combined to create an organized presentation of the comprehensive scope of the conference to generate usable knowledge based on the expertise of panelists and keynotes.

Key Themes

- Uncertainty in an increasingly complex international security environment
  - threats undermining the Rules-Based International Order (RBIO)
  - loss of credibility in the Western World
- The threat is evolving – emerging actors and new domains of warfare
  - hybrid warfare creating greater instability
  - changing character of conflict
  - China's expansion and new cooperation with Russia
- In the information / cognitive domain, everyone is a potential combatant / target
- Defining Canadian national interests in multiple contexts / threats – Canada's role in the world
- Adaptation and innovation in responses to risks, threats, and challenges ~ new partnerships engaging academia and industry partners to generate new ideas, perspectives, and solutions
- Evolution of North American and Arctic defence
  - continued CAN-US cooperation is key
- Evolution of alliances and partnerships, NATO, NORAD, and Five Eyes
- Where does the U.S. fit in geopolitical regions (such as the Middle East)
- New approaches to procurement to fit with new operational requirements – innovation and creativity (operational focus for acquisition process)
- Trusting allies and partners with new technologies that might be compromised (5G issue)
- The character of conflict has changed, but the nature of conflict remains the same ~ human interaction

Context: The Changing Global Security Environment

The sessions addressed current and emerging risks, threats, and challenges to and in the international system within the context of a changing global security environment. Developments in various geopolitical regions were explored, in addition to evolving tactics, networks, and technological capabilities that transcend geographical borders. New domains of warfare, such as cyber, space, and information, create new challenges as they constitute both tools and targets.

The complexity of threats and challenges posed by new and old actors, traditional and non-traditional threats, emerging domains and methods to target the West is leading the world into a period greater instability characterized by: a shifting balance of power, great power competition, rapid evolution of technology across domains, the emergence of "super weapons", and the challenge of resilience in Western democracies. Notably, the primary threats to the Western Liberal Order are Russia, China, and the Trump Administration. The latter concerns whether Trump, and the U.S. as a whole, is a reliable ally.

In the Middle East, new drivers of instability are the protest movements in Lebanon and Syria, the potential for a surge in Iran (in addition to its persistent economic and social problems), and the political limbo that has

enveloped Iraq with no solution in sight. The future of the regime in Syria remains uncertain in light of the economic pressures on Assad, a renewed insurgent campaign, and the likelihood of another refugee movement into Europe. Experts predict a regional vacuum to emerge. As a non-traditional security threat, the COVID-19 crisis poses a risk to human security in Syria, with limited access to health care and humanitarian aid.

Key trends in the Middle East are an active citizenry, loss of faith in institutions, and movement towards hybrid wars – all of which combine to create a significant problem. New challenges concern who is the enemy and who is an ally, and how problems occurring in one place may provide solutions in another. These problems include the continued threat of terrorism, in which the ongoing "war on terror" "takes in energy and spews out other problems," particularly refugees. Terrorists have no accountability, no rules of conduct, and may deploy state-grade capabilities. This contributes to the risk of failed states or states on the brink of failing, such as Syria, Lebanon, Jordan, and Yemen. State responses involve a collapse of norms, involving the use of chemical weapons, shelling civilian populations, and the reckless use of advanced weapon systems.

Russian aggression is one of the primary strategic challenges facing the West. Russia's employment of Hybrid or Grey Warfare leverages multiple domains, especially the information domain (which intersects with cyber). Russia has effectively discovered and targeted Western weaknesses using these new methods, demonstrating a methodological distinction from Soviet propaganda techniques. Putin's intention is to create a false impression of military power. In terms of its capabilities, experts suggest that hypersonic weapons are not much more dangerous than conventional forces. Rather, the primary threat is Russia's aim to destroy Western Liberal Order, which is also a threat to Canada. Russia's developments take advantage of limitations in our defences, but it remains unlikely that Russia would outright attack North America.

Putin is unlikely to retire and has established a succession plan of restructuring so that he can remain in control. This has never been done before and creates new vulnerabilities. He has created an aggressive ideology in Russia within a generation of leaders that believe in it. These followers are likely to be less pragmatic and more aggressive than Putin. Ironically, it is better for Putin to stay in power than Russia to undergo a transition in leadership.

The concern of the West is whether Russian special operations forces (SOF) will act in the Baltics like they did in Ukraine to foment insurgency that Moscow can manipulate. This would require NATO to treat Russian aggression through Article V, while Russia operates at the lower end of Article V. In a military conflict that would involve intervention by Western forces, the Baltic states would likely defend their own countries without waiting for permission. This concerns what Canada's role would be if such a situation emerged. How would Canada act under horizontal escalation?

Russia's goal in Eastern Europe is to sow confusion, a false narrative, and isolate countries (such as Latvia or Ukraine), perhaps spinning a narrative so that NATO will not come to that country's defence. Such actions will not wait until Russia launches an invasion, but will start with information operations that attack the core principles of the Western liberal order. Why is Russia taking these aggressive measures? Russia has not accepted the outcome of the Cold War or the sovereignty of the nations of the former USSR. Challenges in light of this position include Russia's permanent membership in the United Nations Security Council (and China's, for that matter) and what to do with member states who stop conforming.

China is a rising peer-competitor to the U.S. and the West. It poses a challenge to Canada as it seeks to establish a foothold in the Arctic. In light of the Arctic component of its Belt and Road Initiative (its "Polar Silk Road"), China is embarking on cooperation with Russia in developing technologies and pursuing economic opportunities. Furthermore, through Belt and Road economic investment, China has procured financial debt from other countries that it can use to exercise control and leverage. According to one panel official, China "plays positive and constructive role" in the Middle East, with Iran, Sudan, and Syria. It provides peacekeepers, escorts in the Strait, and a new security architecture. Regarding human rights abuses, China claims no abuse of Muslims in the Xinjiang region – a claim that this official discredited as examples of Chinese "fabricated" and "distorted reports."

Other experts identify China as the greatest long-term strategic threat to global security, seeking to change RBIO to create a new order and new relationships centred around the party in Beijing. China bullies other states to accommodate its interests pursued through multi-dimensional tools. Its interests are more important than international law, and it exhibits an authoritarian vision of the future. Its challenge to the American RBIO intensifies competition in the Pacific, in which the U.S. responds with attempts to impose costs on the Chinese military and deny China's objective.

Iran was briefly addressed in terms of the threat posed by proxies in arenas outside of Iran. Although not explicitly stated in the discussions, these include Hezbollah in southern Lebanon, the Houthis in Yemen, and Iran's support to the Assad regime in Syria. These proxies take the battle away from Iran's borders and allow it to influence Middle Eastern dynamics. Additional threats against nations in the region include Iran's ballistic missile and PGM program, and its Quds Force. Iran's nuclear program is also problematic for the future of arms control in the region.

Arms control contributes to peace and security, but experts state that it is not the end of our strategy. The challenge is how to enforce treaties. Russia is not in compliance with arms control; it has violated the Intermediate Nuclear Forces (INF) Treaty since the Obama Presidency. In consideration of the modernization of arms control, what should be integrated into the treaty? Intelligence sharing plays an important role in arms control, recently in sharing information with the Baltic states on Russia's actions and capabilities. In spite of INF violations, both the U.S. and Russia are in compliance with New START. Should cyber be treated like other threats in revising arms control? The U.S does not want cyber as part of arms control because it restricts freedom of information, entrepreneurship, and ideas. This leaves a gap in regulating responsible activities of nation- states in cyber space.

The demise of expertise was identified as a growing issue, described as an erosion from within the rise of populism. The cause and effect involve people's access to media which emboldens them to "know things" and allows leaders to simplify issues, providing no depth and easy answers to difficult questions. This leads to bad

policymaking based around sloganism and echochambers. This also leads to loss of faith in institutions and a confidence crisis in experts and professors whose credibility is being undermined.

New Domains and the Future of War

In anticipating the future of war, it is important to understand and address the types of threats posed by the new domains of cyber, information, and space.

The domains of cyber and information are different but related, as cyber affects the security side and allows for the rapid spread of dis- and misinformation. In Israel and China, cyber is a surveillance technology posing a privacy problem, which works against democracy. In the realm of hybrid warfare, new technologies are cheaper and deniable. States use this new arena to their own advantage in which they exercise no moral high ground to achieve their interests. Notably, Hybrid War is described as a new frontier providing low cost and high payoffs through the use of technology that is both cheap and deniable. The effects "trickle down to every aspect of our lives."

Is the West ready for 5G? Cyber poses an assured IT problem. It marries intelligence and cyber operations, requiring people who understand military and cyber operations, particularly for how we defend the domains and set up defences from a specific threat vector. We need to think differently about how we defend cyber space. Cyber networks and people are getting smarter, posing various non/trans-national actor/individuals threats – and the threat is everywhere. The training of engineers and military operators in this domain is important. We need to understanding the techniques for using a social role for influence and propaganda. There is a significant rise in the volume and sophistication of attacks and the internet infrastructure is a target.

Are we losing the cyber battle? This requires consideration of what winning the battle means. The response involves consequence management – addressing damage or data breaches. How does one measure success? This requires cyber hygiene, cyber intelligence, and cyber resilience. Experts suggest that we are winning and losing the battle at same time. We need insight to better predict threat vectors – a threat index to know the current state, know other actors that are operating in the domain, and share threat insights amongst allies. We need to adopt new techniques and invest smartly.

Cyber attacks tend to go after defence targets, which need to be detected, isolated, and mitigated. Perhaps we are winning, but we are "one click away from losing."[4] Experts note that we are in Phase 2 or 3 of warfare in cyberspace. The risks include a small number of attacks that are very sophisticated (state-sponsored attackers) and the threat is changing – before this, the threat was technical but not hybrid. Today cyber space is filled with operations in many dimensions, including propaganda and psychological operations. In this domain, China is a bigger and more technically-sophisticated threat than Russia; and a large percentage of the cyber threat is from organized crime.

In the private sector China poses a significant security problem as it produces many of the materials – the parts and components – of the electronics that we use. This poses a challenge to supply chain integrity; during material transportation components can be modified. In addition, who is watching our use of technology? Alliance issues concerning the Five Eyes and the challenge of Huawei to 5G uses among intelligence partners are discussed below. Notably, experts describe the challenge posed by the European position, in which many countries chose not to ban Huawei. It was suggested that no 5G provider should be trusted, not just Huawei. The 5G world is difficult to

test and is updated constantly – the speed and velocity of scale is a significant challenge. Quality assurance is critical to ensure that the system is not being used by an adversary. We need to be ablet to trust in the companies involved and transparency in code of scripts. Security operations need to be continual via monitoring, tracking, and alerting. The emergence of quantum computing makes the problem more complex and challenging. The adversary plays by a different set of rules than we do - how do we deal with that? Security must be done as a team, through partners and allies. We need an understanding of points of failure – single points of failure – particularly vulnerabilities of old legacy systems (such a public services and DoD systems). Industry must also identify weakness and upgrade their systems.

War in the future involving new domains concerns the surge in artificial intelligene (AI), robotics, and advanced systems – a new Machine Age compared to the Industrial Revolution. These new technologies bring positives and negatives, including the replacement of people, which introduces new legal, ethical issues, and dilemmas. What responsibilities should be delegated to what machine? Technologies introduce new vulnerabilities, change the nature of cyber threats, create new ideologies, and potentially give rise to new forms of extremism. Big changes are not necessarily in the distant future. AI is difficult to define and we often focus on the wrong issues (such as "killer robots"). Terms and definitions of AI being purchased by leadership remain uncertain with concerns about how to manage the slow understanding of technology. In this realm are we facing a new kind of arms race? This relates to have and have-not states, which creates advantages and disadvantages. The proliferation of AI parallels other game-changing technologies, which need to be addressed in doctrine, i.e. how should we be prepared for conflict with ISIS and other types of groups?

In reference the book *Like War*,[5] one expert identifies hacking networks as a concern – hacking people in media – which has real world effects in the information/cognitive domains. Russia, ISIS, and far right extremists use closed networks, which are more difficult to track. Interestingly, companies are learning from militaries and from red-teaming activities about how an adversary will operate. Companies need to consider how someone will deliberately mis-use a product.

Deep fakes are a significant concern and fall in two general types: 1) taking something real and faking it; and 2) creating something out of nothing, but with a realistic feel. These can be weaponized. On the other hand, malign actors can deny real media by claiming "it was faked" and changing the narrative - "it was manipulated." This increases the challenge of ambiguity in countering deep fakes and their effects, particularly what is real and what is fake. DARPA is working on keeping ahead of detecting manipulation. It was suggested that watermarking should be required to identify real versus fake, with evidence.

The challenge with countering such threats is that adversary states like China will have built-in systems – firewalls and asymmetrical systems to keep out trackers, so that we would not be able to reach into their society as they can to our society. There are lessons to be learned from other nations with experience that have built resilience (like Estonia).

The US has a cyber strategy, but there is a gap in the information domains that utilize social media. Fake news poses educational challenges and opportunities from a public health perspective. In China, there is profit to be gained from fake news, particularly its response to COVID-19 through censorship and disinformation (that the

virus is a "secret bioweapon"). This approach allows for blame casting and false positive news that there is "nothing wrong." It is also possible that in the U.S. manipulation of information about COVID could be used to suppress voters. This is frightening forward-looking, given that this discussion was presented on March 5 and the challenge to American voters in April (physical voting versus voting by mail – implicating the current U.S. Administration's constraints on the U.S. postal system under the current crisis).

How does deterrence apply to social media manipulation, which is a low-cost activity with high gains. In order to threaten punishment – to deter – we must find things that the adversary cares about. What does the adversary fear? What does the adversary ban discussions about? It is important to find their leverage points. It is also helpful to use denial through resiliency language rather than disabling systems. Ultimately, the internet is a tool accessed by everyone, and everyone is a target – we can all be combatants. The new battleground is social media. We are never going to stop cyber attacks or the weaponization of social media, therefore we need to stop focusing on a silver bullet to win and focus on good risk management to reduce its effects.

Canada's Role at Home and the World

This panel considered how Canada can achieve its national interests in an era of great power competition and Canada's role in competition below the threshold of conflict. At the same time Canada must continue to respond to the threat of terrorism and consider how to do counterterrorism "smartly" through security agencies, intelligence, and law enforcement.

As a middle power Canada must interact and engage with the world, but not be coerced. Canada needs to be secure in North America so it can be secure in the world. Since the Cold War Canada maintained a tradition of punching above its weight. Canada's experience in the Baltics has been responding to horizontal escalation, with the CAF training as it fights.

What is Canada's role in the Middle East? One session noted that extremist groups have second and third order destabilizing effects: the displacement of (vulnerable) people, targeting critical infrastructure, destabilizing local and global economies, inflicting resource demands on militaries, and distracting from more pressing threats. Should Canada invest more in this region? It could have long-term payoff such as preventing a void that could collapse, suck in nations and spew out other problems.

It was suggested that Canada is failing to respond adequately to the threat from Russia, as a result of not seeing the effect of Russian activities on the daily life of Canadian citizens. This has a generational component. The experts indicate that Canada's response to Russia must involve strategic communications. Canada must recognize that it is in a better economic and demographic situation than Russia. It must recognize that "we are already in a war with Russia," but that we fail to recognize the grey zone conflict already in progress. Canada is not pushing back when it should be due to "grand strategic gaslighting" and "gaslighting ourselves," based on the belief that it is too difficult or dangerous to push back. Notably, Canada needs to impose costs that Russia cannot bear. Canada has opinions of what the world order should be, but it is not doing anything to achieve or enforce it.

North America and Arctic Defence

The defence of the homeland is critical. The role of the CAF is to defend Canadians at home and abroad, including providing disaster response. Collective defence is important and Canada is no longer the safe haven it once was.

Panelists noted that North America is no longer a sanctuary in the 21st century, as it is subject to broader risks and threats developing in other parts of the globe. Considerations in the emerging global security context involve the modernization of NORAD, the CAN-US relationship, Canada's role in the world, and the capabilities that the CAF can deploy at home and abroad.

It was emphasized that there needs to be a discussion about the relevance and modernization of NORAD. Questions under consideration include how much of NORAD needs to be renewed, and what instruments are required to replace or upgrade technology (particularly the North Warning System built in the 1980s). The experts stated that the evolution of North American defence through NORAD and NORTHCOM requires a holistic approach to close gaps and seams, including cyber defence across networks and new concepts for bilateral cyber defence. It was noted that there is no simple recipe for modernizing NORAD, and it was suggested that NORAD is not the only solution -- although no other options were presented.

Since the Cold War Canada has adapted to changes in the evolution of NORAD. In keeping defences relevant, the focus is moving to the Arctic. The Arctic is a region, a place, and an avenue of approach to our continent. Canada must be prepared for a major disaster, including Northern communities which are in harms' way.

In addressing concerns about Canadian sovereignty and security, the discussion articulated Canada's need to operate further North, which requires infrastructure and multipurpose capabilities across government. It was also stated that "there is no NATO in the Arctic" – what the panelist probably meant is that NATO has no explicit direction or policy specifically on the Arctic,[6] but there may be opportunity or requirement to assume such a posture in the future.

Critical Capabilities

With the emergence of new technologies and generations of capabilities Canadian defence requires growth and innovation. Relationships between government, industry, and academia facilitate this objective, particularly with the DND MINDS program[7] funding academic networks, accessing diversity, talent, and skills.

The Canadian military is about conflict prevention and management, and its preferred tool remains deterrence. It is best to avoid conflict, manage conflict to prevent its spread, and successfully terminate conflict if it cannot be prevented. The ultimate desired outcome is peace and security. However, stability is an illusion if it must be defended at gunpoint all the time. Actions must be aligned with values and Canada has a duty to uphold the laws of armed conflict. We are in a global fight for our values in all domains.

The CAF is mandated to deter by sea, air, and land. It must improve its operationality and meet its requirements outlined in *Strong, Secuire, Engaged* to be strong at home and secure North America. Emerging threats from space, aerospace, maritime domain – above and below water, and new advanced conventional missiles can potentially harm Canadians and critical infrastructure. The CAF and Canada as a nation must be resilient.

The freedom and security of the rules-based international order (RBIO) is threatened daily as our adversaries – particularly Russia and China – grow their spheres of influence to reshape the global order. Both nations use their military forces to destabilize regions, below the threshold of conflict and thus avoiding kinetic operations. This is not sustainable, and the risk of escalation must be prevented in regional and global conflict. Thus deterrence is more than a presence or show of force – it must be credible and offensive and utilize all tools of national power.

Deterrence through offensive capabilities requires agile innovation and the harnessing of new technologies. As warfare is changing, more is needed, including new ways of deployment. 21st century warfare requires flexibility and choice in capability to adapt to the new spectrum of competition and conflict that no longer reflects a simple binary of war and peace. Under these conditions, dynamics can change quickly and we must be ready for any contingency and any threat.

Offensive operations are recommended for Canada to repond more effectively to Hybrid Warfare. This approach involves a "three methods hybrix": offensive, defensive, and counteroffensive. Most people believe the original narrative in information operations, so the challenge is how to tell the truth to achieve a better response and put a country like Russia on the defensive (a position it prefers to avoid).

Russia poses the greatest threat in the physical space, experts suggested, whereas China poses the greatest threat in cyber space. Conventional competitiveness require digitization in investing in the other domains – human capital, medial, logistics, engineering, bandwidth, and conventional force enablers. One expert argues that defence spending should be pegged at 3% of GDP, not 2%. Strategic homework is not just about the money. Capabilities must be set to achieve outcomes through building capacity. This includes the modernization of NORAD and continental defence. Canada could spend more on defence, but it is up to the government and the people to make the decision on what it wants. The challenges for the CAF in this context is attaining skill sets, force structure, force capability – training and resources, including Reserves.

In this new context the CAF is learning and adapting with new capabilities and structures for cyber, space, counter-unmanned aerial systems, and digitization. A lexicon is needed to facilitate common understanding of terms that might mean different things to different audiences. Canada has limited military resources that must be considered in determining what it can deploy and what it should keep at home. Furthermore, for some emerging capabilities – cyber, space, and information – geography does not matter. Integration, precision in delivering effects, and speed and depth are vital. Decision making must be empowered down the ranks, necessitating more education of CAF personnel. There must be blended solutions – human and machine.

The issue of the formulation of CAF priorities in the absence of foreign policy was addressed. One expert indicated that decisions about where, how much, how, and what, will be made in the moment: "We need to know what the capacity is before sending it."

National interests are important to articulate to the public and inform decision making. Canadian security interests in the current context include: great power rivalry, the changing fluid nature of the international order and how it might evolve, subversion through media and election interference, and corruption which creates a lack of faith in institutions. Canada's contribution can include fighting corruption, investing in institutions to make us more resilient, and investing in preventive measures against radicalization. In building capacity, DND should invest in defence diplomacy. To do so, Canada needs a foreign policy agenda that matches *SSE*. This is challenged by various constraints, including the defence and foreign policies of the U.S. and other nations, Canada's own biases and baggage, and Canada's tendency to underperform and undersell itself. However, Global Affairs Canada (GAC) and National Defence have strong links. Canada could leverage its leadership more in Latvia and in the Arctic Council. In the long term, mediation and dialogue will yield successes.

Canada tries to do a lot on the cheap and the question was raised whether we are riding on the coat-tails of past investment. Canada needs to invest more in international affairs and have a voice. Part of this investment involves the DND MINDS program which engages academic expertise to inform Canadian defence policymaking concerning the domestic and international realms.Experts noted the value of rebuilding diplomatic capability at GAC and articulating our national interests. Ultimately Canada's global interests are: predictability, global norms, economic prosperity, securing the country, securing the population, sovereignty, securing North America, and encouraging and supporting an open and stable international system.

Recruiting for Talent

A discussion on CAF recruitment addressed recruiting and retaining the future soldier. There are direct and indirect costs of military attrition. CAF service is a unique career that entails tradeoffs in lifestyle choice (as military families make sacrifices). Individuals' decisions to remain in the CAF are complex. Challenges to recruitment include acquiring talent, gaining, and retaining talent, particularly among Millennials. Thus, in alignment with *SSE*, the CAF is pursuing a retention strategy with a relational approach, seen to be more effective than the transactional approach. Enablers of retention include: flexibility and member choice, options, leadership at all levels, and understanding the drivers of healthy and unhealthy attrition through anecdotal research. A new retention culture will address key issues such as families, career, challenges, and opportunities. Families are emphasized in terms of addressing alternative career paths with create changes in life and families, which might affect career priorities. Family support includes spousal career support and training. Ultimately, CAF recruitment emphasizes the value of diversity, which brings different experiences, backgrounds, perspectives, ethos, and skills. Embracing diversity is essential to meet emerging needs for cyber operations, information operations, and space. The CAF needs to change and adapt in order to recruit the future fighter.

The panelists addressed Canadian procurement issues, including in the context of its relationship with the U.S. and U.S. pressures for Canada to spend more on defence. Differences in procurement processes were addressed at length in terms of Canadian assumptions of U.S. approaches and procedures, and how these shifted with changes in the security context from a focus on terrorism to near-peer competitors. In this way the U.S. approach involves the alignment of goals and objectives with its national defence strategy to create an effective warfighting

military force. It acknowledges the importance of Canada to the U.S., as it never fights alone, but involves support from partners and allies.

U.S. procurement concepts emphasize innovation and agility, considering future challenges, and determining how to succeed with required capabilities. The level of complexity involved in procurement at DND was addressed in light of responsibility and accountability to Canadian citizens and the CAF. The U.S. approach was compared to the Canadian in terms of shifting how it engages with the public and expert community, implementing laws/policies/practices for acquisition, and being cognizant of the media which watches and reports on acquisition processes. These variables lead to acquisition professionals being risk-averse. Understanding these challenges has led to new approaches, such as the Adaptive Acquisition Framework, which simplifies core policy and functional areas.

The challenge that technology moves at a faster pace than acquisition cycles affects both the U.S. and Canada, necessitating moving at the speed of relevance. Thus, the U.S. is exploring innovation by engaging small companies and non-traditional DoD suppliers. In Canada, the DND IDEaS[8] program also seeks innovative solutions to address CAF needs. Such programs seek more open-ended approaches, including "finding solutions to a problem you didn't know you had." Such programs also include partnerships with allies to share insights and best practices to adapt and move forward. Challenges to innovation include needing a capacity but not knowing the specifications. New processes are needed to help with prototyping and fielding a capability, or investing in a current capability to meet requirements. "Creative compliance" requires critical thinking that will facilitate fielding an innovative solution – i.e. getting the capability off the range and onto the battlefield. The U.S. faces similar challenges to Canada in terms of getting well-defined guidance from the Joint Chiefs of Staff, with the Administration often holding back innovation.

The discussion involved the cyber security issue. We are "at cyber war every day," with implications for both national and economic security. This includes challenges in cyber security when partnering with academia and small companies, as well as larger industry partners that need to be cyber certified. Dealing with both classified and unclassified information raises issues of access. Vetting and developing trust with partners to develop specific kinds of capabilities / weapons must also factor in how much foreign technology (such as 5G) is involved in defence systems. China has articulated its plans to dominate by 2025, and this involves getting the intellectual property (IP) and capability to compete by any means. Through deploying adversarial capital, China seeks (through shell companies) to acquire businesses in the U.S. that have technology critical to national defence. How can the U.S. block, firewall, or undo acquisitions by adversaries? Furthermore, when leveraging innovation by investing in university research, DoD must be careful to vet the graduate students involved, particularly students who may take IP back to China where U.S. defence-funded research might be used against us.

DND is also seeking solutions to similar challenges in evaluating players in the procurement process. As it is accountable to taxpayers, the Canadian government seeks adaptive solutions through diversity and social responsibility.

Alliances and Partnerships

Alliance relationships are changing in the current era of complexity. Examining a strategic issue requires looking at the world at large.

NATO resilience is based on shared Western values and interests, comprising the backbone of the RBIO. It is now operating under new paradigm as a result of the threats from China, Russia, terrorism, and pandemics. However, it is a mistake to stretch NATO's Area of Responsibilty. It is important to match resources to capabilities in the Alliance. NATO is committed to the Indo-Pacific region and the range of threats posed by climate change and freedom of navigation to the international security and defence community. The region is seeing an almost permanent military presence in the maritime domain with the carrier strike group. By comparison, capabilities in the Atlantic and Pacific have atrophied due to the campaigns in Afghanistan and Iraq. Securing the North Atlantic from the Russian threat should be NATO's priority.

Experts stated that Russia wants to drive a wedge into the Alliance but will never be able to do this because the Alliance is strong. The West needs to push back against Russia's adventurism around the world. Notably, in a time of increasing instability, the US and its Allies can do a great deal to shape the trajectory of stability and security.

Applying military power requires frank discussions about operational costs, rebuilding expertise, and awareness of risks and opportunities. One issue addressed was whether NATO enlargement impeded its ability to succeed in its mission. This discussion considered security providers versus security consumers. NATO is a political alliance, however, and not every member needs to do all military things; rather, it should take broad view of the contributions by member states. Considerations about how to modernize the alliance addressed how it could more effectively draw upon niche activities for some countries – for instance, more SOF for some, more cyber for others. This would help to leverage various types of operational niches or breadths that can be provided, which in some cases are geographically-dependent. Different contexts will yield different portfolios.

The Five Eyes intelligence sharing relationship provides advantages – a special membership based on trust and the defence of values. The issue of Huawei (viewed as a hostile vendor) providing 5G in some member states prompted the question of possible expulsion from the Five Eyes. Information sharing also represents a sovereignty issue that involves all domains of information (eg. economic, personal, national security). Furthermore, the discussion highlighted that information is perishable in today's world – it has a limited shelf life.

Operational Approaches

The operational environment is rapidly changing, requiring a rethink of defence and security posture. New concepts to meet today's battlespace include multidomain integration, a layered integrated approach, and deterrence of conventional conflict involving operating below the level of conflict (sub-threshold). How much and what kind of investment is needed to deter our adversaries? NATO needs to mobilize in preparation to fight tomorrow. In terms of readiness it will take years to reach operational capability, but the talents people bring are

richer today. Requirements include offensive and defensive cyber warriors, bringing intelligence and information into a cloud architecture, and the ability to exploit data at the right time and place.

One expert outlined four key focus areas to guide strategic objectives for moving forward: 1) increasing joint and combined force lethality through investments in leading edge technology and new methods of coercion; 2) enhancing designs for when and where we operate in all domains (such as more advanced radar, missile defence, and Command and Control (C2) systems); 3) advancing exercises for innovation, modernization, integration, experimentation, and joint C2; and 4) strengthening allies and partners to enhance capabilities and coordination through regular exercises and training. The envisaged end state is an integrated coalition, operational across all domains to dissuade adversaries from military action.

Conclusion

This report outlines experts' perspectives on how Canada and its Western Allies understand and respond to defence and security risks, threats, and challenges posed by traditional and non-traditional actors across multiple domains. Discussions at the Ottawa Conference on Security and Defence addressed issues that coincide with various goals outlined in *Strong, Secure, Engaged* to anticipate, adapt, and act. From a national interest perspective, the deliberations offred various considerations about how Canada should respond in various geographical regions and domains, and how the CAF must evolve alongside emerging or changing threats by developing innovative solutions and integrating its systems. Defence and diplomatic engagement in the world requires foreign policy guidance, and effective responses within alliance frameworks involve action at multiple levels.

This report identifies various gaps that should be addressed in greater detail. The first is the question of Canada's potential participation in Ballistic Missile Defence. The subject was broached during a question period, but not adequately addressed by panelists. Another issue is the difficult discussion regarding potential nuclear threats in the event that conflict escalates in Eastern Europe between Russia and the Baltic states. This potentiality has implications for both NATO writ large (the credibility of its extended nuclear deterrence for allies) and for Canada, given its particular role in the nuclear alliance. What role might Canada play as a mediator to encourage stability and de-escalate a crisis?[9]

A final thought considers the evolution of the COVID-19 situation. This conference, held in early March, preceded the full-blown COVID-19 crisis by mere days. Although experts presented preliminary analysis and projections of the potential threat that this pathogen presented in certain geographical regions, there is an opportunity to evaluate these projections under current and developing conditions.

Annex I: Conference Agenda[10]

OTTAWA CONFERENCE ON SECURITY AND DEFENCE

MARCH 4-5 2020

FAIRMONT CHÂTEAU LAURIER
OTTAWA, ONTARIO

STICKHANDLING THROUGH ROUGHING AND INTERFERENCE: HOW TO POSITION CANADA IN THE GREAT POWER PLAYS

SPECIAL EVENT - BEFORE CONFERENCE	
08:00 - 17:00 KPMG	ANNUAL GENERAL ASSEMBLY OF THE CONFERENCE OF DEFENCE ASSOCIATIONS (BY INVITATION ONLY)
17:00 - 19:00 CHATEAU LAURIER	BOOK LAUNCH: CANADIAN DEFENCE POLICY IN THEORY AND PRACTICE (ED. T. JUNEAU, P. LAGASSE, S. VUCETIC), HOSTED BY THE CANADIAN DEFENCE AND SECURITY NETWORK
DAY 1 - MARCH 4TH	
07:00 - 8:00 ADAM CORRIDORS	REGISTRATION
08:00 - 08:15 BALLROOM	OPENING - LGEN GUY THIBAULT (RET'D), CHAIR OF THE CDA INSTITUTE
	CONFERENCE CONCEPT & SETTING - DR. YOURI CORMIER, EXECUTIVE DIRECTOR OF THE CDA INSTITUTE
8:15 - 8:30 BALLROOM	DEPUTY MINISTER OF NATIONAL DEFENCE MS JODY THOMAS (IN LIEU OF HON. HARJIT SAJJAN, MINISTER OF NATIONAL DEFENCE
8:30 - 10:15 BALLROOM	SESSION 1 - ESCALATING OR DE-ESCALATING WITH RUSSIA RELATIONS: NORAD MODERNIZATION, FORWARD PRESENCE & REVAMPING THE ARMS CONTROL TREATY ARCHITECTURE
	MODERATOR: MERCEDES STEPHENSON, OTTAWA BUREAU CHIEF, GLOBAL NEWS OTTAWA
	CONVENOR: MATTHEW GRAHAM, CEO OF UNISYNC GROUP LIMITED
	SPEAKER: HON. ANDREA THOMPSON, FORMER US UNDER SECRETARY OF STATE FOR ARMS CONTROL & INTERNATIONAL SECURITY
	SPEAKER: LGEN CHRISTOPHER J. COATES, DEPUTY COMMANDER, NORAD
	SPEAKER: JANIS GARISONS - STATE SECRETARY OF THE MINISTRY OF DEFENCE OF LATVIA
	SPEAKER: DR. FREDERICK KAGAN, AMERICAN ENTERPRISE INSTITUTE – CRITICAL THREATS
10:15 - 10:30 LAURIER ROOM	HEALTH BREAK
10:30 - 12:00 BALLROOM	SESSION 2 – GREAT POWER DYNAMICS IN THE MIDDLE EAST
	MODERATOR: MURTAZA HUSSAIN, JOURNALIST, THE INTERCEPT
	CONVENOR: MME FRANÇOISE GAGNON, CEO, ADGA GROUP
	SPEAKER: AMBASSADOR CONG PEIWU, AMBASSADOR OF THE PEOPLE'S REPUBLIC OF CHINA TO CANADA
	SPEAKER: COL AMOS NACHMANI, MILITARY ATTACHÉ, ISRAEL EMBASSY IN CANADA
	SPEAKER: JENNY CAFARELLA, RESEARCH DIRECTOR, INSTITUTE FOR THE STUDY OF WAR

12:00 - 13:00 DRAWING ROOM	LUNCH BREAK
13:00 - 15:00 BALLROOM	**SESSION 3 - GLOBAL TRANSATLANTIC COOPERATION**
	MODERATOR: DICK FADDEN, FORMER DIRECTOR OF CSIS, DEPUTY MINISTER OF DEFENCE & NATIONAL SECURITY ADVISOR
	CONVENOR: LOUIS BIBEAU - COMPANY FOUNDER AND CEO, LOGISTIK UNICORP INC.
	SPEAKER: LGEN ROBERT MAGAWON, DEPUTY COMMANDER STRATEGIC COMMAND (IN LIEU OF ADM TIMOTHY FRASER, UK VICE CHIEF OF DEFENCE STAFF
	SPEAKER: ADMIRAL PHILIP DAVIDSON, COMMANDER, U.S. INDO-PACIFIC COMMAND (PACOM)
	SPEAKER: VADM HENRI SCHRIKE, HEAD OF INT. AFFAIRS, FOR THE ÉTAT-MAJOR DES ARMÉES, FRANÇAISES
	SPEAKER: LGEN MICHAEL ROULEAU, COMMANDER, CANADAIAN JOINT OPERATIONS COMMAND (CJOC)
15:00 - 15:15 LAURIER ROOM	HEALTH BREAK
15:15 - 16:00 BALLROOM	PRESENTATION + Q&A : GENERAL JONATHAN VANCE, CANADIAN CHIEF OF DEFENCE STAFF
16:00 - 16:15 BALLROOM	NICHOLA GODDARD AWARD PRESENTATION
16:15 - 18:00 LAURIER ROOM	RECEPTION COCKTAIL
DAY 2 - MARCH 5TH	
09:00 - 10:00 LAURIER ROOM	REGISTRATION
CONTINENTAL BREAKFAST	CHAIRMAN'S CIRCLE: MEET NEW LEADERSHIP (GUY THIBAULT/YOURI CORMIER) AND MEMBERS OF OUR BOARD
10:00 - 11:15 BALLROOM	**SESSION 4 - DESIGNING PROCUREMENT: FUTURE CHALLENGES & GETTING THE RIGHT EQUIPMENT AT THE RIGHT PRICE AT THE RIGHT TIME**
	MODERATOR: PHILIPPE LAGASSÉ, CARLETON UNIVERSITY
	CONVENOR: LORRAINE BEN, CHIEF EXECUTIVE, LOCKHEED MARTIN CANADA
	SPEAKER: TROY CROSBY, ASSISTANT DEPUTY MINISTER OF DEFENCE (MATERIEL)
	SPEAKER: HON. ELLEN LORD, US UNDER SECRETARY OF DEFENSE FOR ACQUISITIONS AND SUSTAINMENT
11:15 - 12:15 BALLROOM	**SESSION 5 - MILITARY PERSONNEL: RECRUITING AND RETAINING THE FUTURE SOLDIER**
	MODERATORS: OFFICER-CADETS ELODIE BÉDARD AND ALEXANDRA ALEXUTA (ROYAL MILITARY COLLEGE OF CANADA)
	CONVENOR: BRYAN BRULOTTE - CEO, MAXSYS STAFFING AND CONSULTING
	SPEAKER: ADM HAYDN EDMUNDSON, COMMANDER, MILITARY PERSONNEL COMMAND
	SPEAKER: CHIEF WARRANT OFFICER J.C.D. GEOFFROY, MILITARY PERSONNEL COMMAND
	SPEAKER: DR. IRINA GOLDENBERG, MILITARY PERSONNEL COMMAND
12:15 - 13:15 DRAWING ROOM	LUNCH BREAK

13:15 - 14:30 BALLROOM	SESSION 6 - CYBER/5G – CRITICAL INFRASTRUCTURE AND BATTLEFIELD THREATS
	MODERATOR: ROBERT FIFE, OTTAWA BUREAU CHIEF, THE GLOBE AND MAIL
	CONVENOR: GRANT J. MCDONALD, GLOBAL SECTOR LEADER, AEROSPACE & DEFENCE; LEAD PARTNER, KPMG
	SPEAKER: RADM DWIGHT SHEPHERD (RET'D), FORMER DIRECTOR - CYBERSPACE OPERATIONS, U.S. NORTHERN COMMAND/ NORAD
	SPEAKER: DR. DIDIER DANET, DIRECTOR - MSC CYBER DEFENCE, MILITARY ACADEMY OF SAINT-CYR
	SPEAKER: DR. SHUE JANE THOMPSON, VICE PRESIDENT AND PARTNER, GLOBAL SECURITY STRATEGY AND GROWTH, IBM
14:30 - 14:45 LAURIER ROOM	HEALTH BREAK
14:45 - 15:45 BALLROOM	SESSION 7 – MOVING FORWARD: HOW IS CANADA TO POSITION ITSELF TO SECURE ITS NATIONAL INTERESTS IN AN AGE OF GREAT POWER COMPETITION AND WARFARE BELOW THE THRESHOLD?
	MODERATOR: DR. BESSMA MOMANI, PROFESSOR, THE UNIVERSITY OF WATERLOO
	CONVENOR: YOURI CORMIER, EXECUTIVE DIRECTOR, THE CONFERENCE OF DEFENCE ASSOCIATIONS INSTITUTE
	SPEAKER: DR. ANN FITZ-GERALD, DIRECTOR, BALSILLIE SCHOOL OF INTERNATIONAL AFFAIRS
	SPEAKER: MR. PHIL GURSKI - PROGRAMME DIRECTOR, SECURITY, ECONOMICS, TECHNOLOGY, UNIVERSITY OF OTTAWA
	SPEAKER: DR BALKAN DEVLEN, ASSOCIATE PROFESSOR, UNIVERSITY OF COPENHAGEN
15:45 - 16:45 BALLROOM	SESSION 8– THE FUTURE OF WAR
	MODERATOR: LEAH WEST L.L.M. J.D., LECTURER, CARLETON UNIVERSITY
	CONVENOR: GARRY VENMAN, PRESIDENT, RAYTHEON INTERNATIONAL CANADA
	SPEAKER: DR. PETER SINGER – 'NEW AMERICA FOUNDATION'
THANK YOU & FAREWELL – EXECUTIVE DIRECTOR, DR. YOURI CORMIER	

[1] CDA Institute, homepage, https://cdainstitute.ca/.
[2] CDA Institute, Ottawa Conference on Defence and Security, https://cdainstitute.ca/conference-on-security-defence-2020/.
[3] CDAI, Ottawa Conference, Speakers, https://cdainstitute.ca/conference-on-security-defence-2020/.
[4] "Bad links" are used to illustrate how we are one click away.
[5] Peter Singer and Emerson T. Brooking, *Like War: The Weaponization of Social Media* (New York: Houghton Mifflin Harcourt Publishing Company, 2018).
[6] Lackenbauer dicusses the absence of the Arctic in the NATO Strategic Concept, although NATO is a key multilateral institution in the Arctic – See P. Whitney Lackenbauer, "Fieldnotes from an Arctic "Bazaar": Report on the 2019 Arctic Council Assembly, Reykjavik, Iceland," NAADSN Activity Report (October 2019): 10, 12.

https://www.naadsn.ca/wp-content/uploads/2020/01/19-oct- lackenbauer-report-on-arctic-circle-2019-for-NAADSN.pdf.

[7] Department of National Defence, Mobilizing Insights in Defence and Security (MINDS), https://www.canada.ca/en/department- national-defence/programs/minds.html.

[8] Department of National Defence, Innovation for Defence Excellence and Security (IDEaS), https://www.canada.ca/en/department- national-defence/programs/defence-ideas.html.

[9] Crisis stability and strategic stability are concepts in nuclear strategy and deterrence referring to conditions under which competitor states are not incentivized to use nuclear weapons against one another. Crisis stability in particular refers to conditions of mutual deterrence that prevent the escalation of a conflict to cross the nuclear threshold. Thomas C. Schelling, *Strategy of Conflict* (Cambridge, MA: Harvard University Press, 1960).

[10] Agenda provided by CDA Institute for dates of 3-4 March 2020, https://cdainstitute.ca/conference-on-security-defence-2020/. (Agenda now no longer posted on webpage).